УДК 004.056.5 URL: https://ptsj.bmstu.ru/catalog/icec/insec/1038.html

ХАРАКТЕРИСТИКА ВРЕДОНОСНЫХ ПРОГРАММ ДЛЯ LINUX: ВЫВОДЫ И НЕДАВНИЕ ТЕНДЕНЦИИ

А.К. Тоноян tonoyanak@student.bmstu.ru
Е.В. Глинская glinskaya@bmstu.ru
SPIN-код: 5430-3023

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

В последние годы наблюдается рост числа вредоносных программ, которые нацелены на инфраструктуры, построенные на IoT-устройствах. В статье представлено исследование вредоносного программного обеспечения, ориентированного на операционные системы Linux и устройства интернета вещей (IoT). С помощью методов статического и динамического анализа классифицированы известные угрозы и выявлены новые. Использован уникальный датасет, собранный сообществом, что позволило провести глубокий анализ тенденций. Среди основных находок: увеличение числа криптомайнинговых атак, рост сложности атак и быстрое появление новых вредоносных программ с минимальными вложениями в инфраструктуру. Данное исследование может быть полезным для специалистов по компьютерной криминалистике и безопасности IoT.

Ключевые слова: вредоносное программное обеспечение, криминалистика, интернет вещей, встраиваемые системы, аналитика данных, машинное обучение, экспертные системы

Введение. Malware, или «малварь» (сокращенно от англ. *malicious software*) — вредоносное программное обеспечение (ПО), цель которого — в той или иной форме нанести ущерб пользователю или компьютеру и его содержимому. Малварь — общее название для всех видов киберугроз, таких как вирусы, трояны, шпионские программы, кейлоггеры, adware и др. Malware, или вредоносы, — достаточно распространенный вид киберугроз, и столкнуться с вредоносным ПО может каждый. В последние десятилетия акцент злоумышленников сместился с операционных систем Windows на системы на базе Linux из-за популярности Linux в инфраструктуре интернета вещей (internet of things — IoT) [1]. Рост числа подключенных устройств (ожидается, что их число к 2030 г. достигнет 40 млрд), также увеличивает риски. Эти устройства с ограниченными ресурсами (память, пропускная способность, энергопотребление) часто не имеют антивирусной защиты, что делает их уязвимыми для атак, таких как создание ботнетов [2].

Кроме того, системы IoT работают на различных архитектурах (ARM, PowerPC, MIPS), что также привлекает злоумышленников. Малварь для Linux,

© МГТУ им. Н.Э. Баумана, 2025 ISSN 2541-8009

направленная на IoT, появилась относительно недавно, и количество известных семейств все еще невелико. Первая крупная угроза — ботнет Mirai, использовавшийся для DDoS-атак, и его исходный код, выпущенный в 2016 г., дал толчок для появления множества новых версий.

Обзор угроз. IoT — это быстро развивающееся образование, состоящее из встроенных и многоплатформенных устройств. Большинство вредоносного ПО для IoT сосредоточено на устройствах с учетными данными по умолчанию, и эти устройства становятся целью недавно обнаруженного вредоносного ПО на базе Linux. В последние несколько лет вредоносное ПО в IoT привлекло больше внимания из-за ущерба, причиненного крупномасштабными атаками, такими как атака, проведенная ботнетом Mirai [3]. Увеличение числа устройств IoT вместе с отсутствием обновлений в условиях появления новых уязвимостей привело к распространению вредоносного ПО, нацеленного на эти платформы. Кроме того, публикация или утечка исходного кода некоторых семейств, таких как Mirai или Bashlite, приводит к появлению новых вариантов или созданию новых семейств, использующих часть их функциональности или методов распространения и заражения новых устройств [4].

Методология исследования. Разработанная нами методология состоит из трех основных фаз: 1) извлечение признаков и моделирование; 2) открытие; 4) проверка. В первой фазе исследования проводят исследовательский анализ для выбора наиболее значимых признаков, которые будут использоваться для обучения классификатора машинного обучения (machine learning — ML). Во второй фазе применяют обученный классификатор для связи неизвестных образцов с известными используя метрики, основанные на последовательностях опкодов. Наконец, в третьей фазе используют кластеризацию для выявления новых угроз, которые еще не были охарактеризованы [5].

Обзор системы. Основные блоки разработанной нами системы показаны на рисунке. Сначала идет фаза извлечения признаков и моделирования. Идея этой фазы заключается в проведении исследовательского анализа, направленного на выявление и отбор наиболее информативных характеристик вредоносного ПО для последующего машинного обучения. После выбора наиболее релевантных признаков в области IoT создают классификатор ML, способный охарактеризовать различные известные угрозы. В фазе открытия используют классификатор, обученный на предыдущей фазе, и метрику, основанную на последовательностях опкодов из дизассемблирования вредоносного ПО, чтобы связать неизвестные образцы с образцами известных угроз. Наконец, в фазе проверки раскрывают новые угрозы, неизвестные сообществу [6, 7].

 © МГТУ им. Н.Э. Баумана, 2025

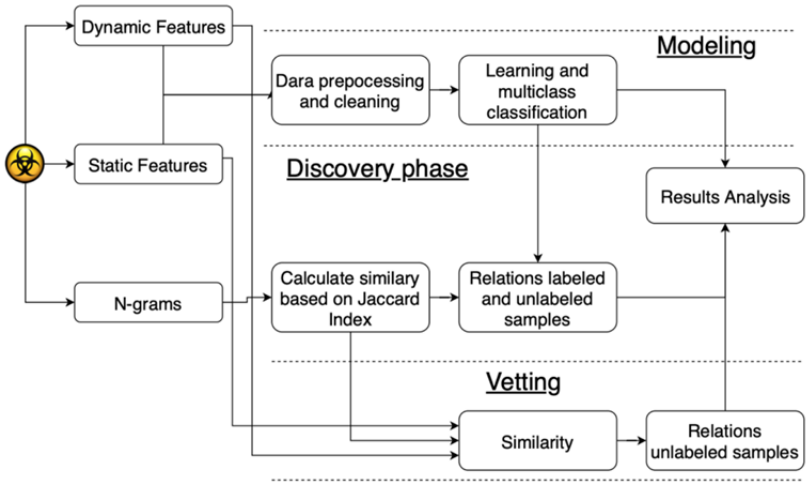

Схема взаимодействия элементов системы:

Denamic Features — динамические особенности; Static Features — статические характеристики; N-grams — N-граммы; Data preprocessing and cleaning — предварительная обработка и очистка данных; Discovery phase — фаза открытия; Calculate similary based on Jaccard Index — рассчитать аналогично на основе индекса Жаккара; Learning and multiclass classification — обучение и многоклассовая классификация; Relations labeled and unlabeled samples — отношения маркированных и немаркированных образцов; Similarity — Сходство; Modeling — моделирование; Results Analysis — анализ результатов; Relations unlabeled samples — отношения немаркированных образцов

Анализ и классификация вредоносного ПО. В ходе проведенного нами исследования был проанализирован наиболее представительный набор данных вредоносного ПО на базе Linux. Было показано, что разработанная нами система может точно охарактеризовать известные угрозы. Эта система была использована для исследования ряда ранее неизвестных угроз [8]. Сначала были идентифицированы известные шаблоны в неразмеченном наборе данных с использованием классификатора, обученного на размеченном наборе данных, а затем полученные признаки были объединены с пользовательской функцией расстояния для обнаружения новых угроз путем кластеризации похожих образцов.

Заключение. Проведенное исследование подчеркивает необходимость разработки более эффективных стратегий обнаружения и противодействия вредоносному ПО, нацеленному на IoT. Результаты исследования помогут в разработке более надежных инструментов для борьбы с этими угрозами. Характеристики, полученные для каждого из кластеров, могут быть полезными для дальнейших исследований в этой области.

© МГТУ им. Н.Э. Баумана, 2025 ISSN 2541-8009

Таким образом, исследование не только предоставляет новые данные о вредоносном ПО, нацеленном на IoT, но и открывает новые горизонты для будущих исследований в области цифровой криминалистики и безопасности [9, 10].

Литература

[1] Alshaer M., Alshehhi Kh., Abdulla S. The Internet of Things (IoT) Forensic Investigation Process. *Journal of Information Security and Cybercrimes Research*, 2023, vol. 6, no. 2, pp. 150–161. https://doi.org/10.26735/dbeu2801

[2] Бударный Г.С., Казанцев А.А., Красов А.В., Поляничева А.В. Разновидности нарушений безопасности и типовые атаки на операционную систему. *Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Междунар. науч.-техн. и науч.-метод. конф.: сб. ст.* Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2022, т. 4, с. 406–411.

[3] Грибунин В.Г., Гришаненко Р.Л., Лабазников А.П., Тимонов А.А. Безопасность систем машинного обучения. Защищаемые активы, уязвимости, модель нарушителя и угроз, таксономия атак. *Известия Института инженерной физики*, 2021, № 3 (61), с. 65–71.

[4] Lahe A.D., Singh G. A Survey on Security Threats to Machine Learning Systems at Different Stages of its Pipeline. *International Journal of Information Technology and Computer Science*, 2023, vol. 15, no. 2, pp. 23–34. https://doi.org/10.5815/ijitcs.2023.02.03

[5] Цветков А.Ю. Исследование существующих механизмов защиты операционных систем семейства Linux. *Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Междунар. науч.-техн. и науч.-метод. конф.: сб. ст.* Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018, т. 1, с. 657–662.

[6] Штеренберг С.И., Бударный Г.С., Чумаков И.В. Анализ безопасности доменных систем. *Региональная информатика. Юбилейная XVIII Санкт-Петербургская междунар. конф.: матер*. Санкт-Петербург, Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления, 2022, т. 1, с. 587–588.

[7] Bai Ya., Wang Y., Zeng Yu. et al. Query efficient black-box adversarial attack on deep neural networks. *Pattern Recognition*, 2023, vol. 133, art. 109037. https://doi.org/10.1016/j.patcog.2022.109037

[8] Зылева П.С., Пестов И.Е., Тремель И.С., Юрова У.С. Методы обеспечения безопасности Astra Linux special Edition. *Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Междунар. науч.-техн. и науч.-*

метод. конф.: сб. ст. Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023, т. 1, с. 553–558.

[9] Горбань С.А., Красов А.В., Цветков А.Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux. *Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Междунар. науч.-техн. и науч.-метод. конф.: сб. ст.* Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023, т. 1, с. 345–348.

[10] Астапов Р.Л., Мухамадеева Р.М. Автоматизация подбора параметров машинного обучения и обучение модели машинного обучения. *Актуальные научные исследования в современном мир*е, 2021, № 5–2 (73), с. 34–37.

Поступила в редакцию 24.10.2024

Тоноян Альберт Каренович — студент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Глинская Елена Вячеславовна — старший преподаватель кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Басараб Михаил Алексеевич, доктор физико-математических наук, заведующий кафедрой «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:
Торонян А.К., Глинская Е.В. Характеристика вредоносных программ для Linux: выводы и недавние тенденции. *Политехнический молодежный журнал*, 2025, № 02 (97). URL: https://ptsj.bmstu.ru/catalog/icec/insec/1038.html

© МГТУ им. Н.Э. Баумана, 2025 ISSN 2541-8009

CHARACTERISTICS OF THE LINUX MALWARE: CONCLUSIONS AND RECENT TRENDS

A.K. Tonoyan tonoyanak@student.bmstu.ru
E.V. Glinskaya glinskaya@bmstu.ru
SPIN-code: 5430-3023

Bauman Moscow State Technical University, Moscow, Russian Federation

In the recent years, an increase is observed in the number of malware programs that target infrastructures built on the IoT devices. The paper presents a study of the malware programs aimed at the Linux operating systems and the Internet of Things (IoT) devices. Using the static and dynamic analysis methods, it classifies the known threats and identifies the new ones. A unique dataset collected by the community is used making it possible to analyze in-depth the existing trends. Key findings include an increase in the number of the crypto-mining attacks, growing attacks complexity, and the rapid emergence of new malware with minimal investment in the infrastructure. Study results could be useful for specialists in computer forensics and the IoT security.

Keywords: malware, forensics, Internet of Things, embedded systems, data analytics, machine learning, expert systems

Received 24.10.2024

Tonoyan A.K. — Student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Glinskaya E.V. — Senior Lecturer, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Basarab M.A., Dr. Sci. (Phys.-Math.), Head of the Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Tonoyan A.K., Glinskaya E.V. Characteristics of the Linux malware: conclusions and recent trends. *Politekhnicheskiy molodezhnyy zhurnal*, 2025, no. 02 (97). (In Russ.). URL: https://ptsj.bmstu.ru/catalog/icec/insec/1038.html

 © BMSTU, 2025